Release Notes for Cisco UCS Rack Server Software, Release 6.0(2)

First Published: 2026-03-16

Cisco UCS C-Series Servers

Cisco UCS C-Series Servers deliver unified computing in an industry-standard form factor to reduce total cost of ownership and increase agility. Each product addresses varying workload challenges through a balance of processing, memory, I/O, and internal storage resources.

About the Release Notes

This document describes the new features, system requirements, open caveats and known behaviors for C-Series software release 6.0(2) including Cisco Integrated Management Controller (Cisco IMC) software and any related BIOS, firmware, or drivers. Use this document in conjunction with the documents listed in the Related Documentation, on page 37 section.

Note We sometimes update the documentation after original publication. Therefore, you should also refer to the documentation on Cisco.com for any updates.

Revision History

Revision	Date	Description
A0	March 16, 2026	Created release notes for 6.0(2.260044) for the following servers: • Cisco UCS C220 M8, C240 M8, C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 6.0

Cisco IMC Release Number and .ISO Image Names

Beginning with the release 4.3, Cisco is updating the release number naming convention to align with the .ISO images.

Example: **4.3.1.YYXXXX**

- **4.3**—Represents the main release.
- **.1**—Represents the first release.

  For the current 4.3 main release, **.1** represents the first release number.

  For subsequent maintenance releases, this number will represent the related maintenance release number.
- **YY**—Represents the year of release.

  For the current 4.3 main release, **23** is derived from the year 2023.
- **XXXX**—The final 4 digits represent the increasing sequence of build numbers every year.

  For the first 4.3 main release, the number is **0097**.

New Software in Release 6.0(2)

New Software Features in Release 6.0(2.260044)

The following new software features are supported in Release 6.0(2.260044):

- Support for mTLS client CA certificate. This feature allows the server to use a Certificate Authority (CA) public certificate to verify the identity of connecting clients. With Mutual Transport Layer Security (mTLS), both the client and server authenticate each other, providing secure two-way verification before establishing a connection.
- Support for Secure Hash Algorithm 512 (SHA 512) authentication in SNMP configuration, enabling stronger, high-assurance security for SNMP communications.
- Support for configuration of MTU values up to 9158 bytes per vNIC in Cisco IMC. This enhancement enables jumbo frame support for advanced networking and storage use cases on Cisco UCS 15000 VIC adapters.
- Cisco IMC now supports up to 16,384 LUNs per vHBA (FC-Initiator) for supported Cisco UCS VIC adapters. This enables better compatibility with modern storage arrays and host OSes supporting large LUN counts.
- Support for NFS over RDMA is available with Cisco UCS VIC 15000 Series adapters on Linux.
- The default values for the Transmit Queue Ring Size and Receive Queue Ring Size settings have been increased to 4096 for all Cisco UCS VIC adapters.

Security Fixes

Security Fixes in Release 6.0(2.260044)

Defect ID - CSCwr50426

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2024-13176—A timing side-channel vulnerability in OpenSSL's ECDSA signature computation may allow an attacker with local access or a low-latency network connection to potentially recover a private key, particularly when using the NIST P-521 curve.
- CVE-2024-5535—A buffer overread flaw in OpenSSL's SSL_select_next_proto API function, triggered when called with an empty client protocols buffer, may cause an application crash or allow up to 255 bytes of private memory to be sent to a peer.
- CVE-2024-9143—Use of low-level GF(2^m) elliptic curve APIs in OpenSSL with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes, potentially resulting in an application crash or remote code execution.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwr81218

Cisco IMC includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2025-48384—A link following vulnerability in Git stems from inconsistent handling of carriage return characters in configuration files; when initializing a submodule with a trailing carriage return in its path, the altered path may lead to an incorrect checkout location, potentially allowing arbitrary code execution if a symlink points to a malicious hook script.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwr83710

Cisco IMC includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2021-0920—A race condition in the Unix domain socket implementation (unix_scm_to_skb in af_unix.c) of the Linux kernel may lead to a use-after-free vulnerability, allowing a local attacker to potentially escalate privileges or cause a system crash.
- CVE-2024-53150—An out-of-bounds read vulnerability in the Linux kernel's ALSA USB-audio driver, caused by insufficient validation of descriptor lengths (bLength), may allow an attacker with physical access to use a malicious USB device to disclose sensitive kernel memory or cause a denial of service.
- CVE-2025-38352—A race condition in the Linux kernel's POSIX CPU timer handling between the handle_posix_cpu_timers() and posix_cpu_timer_del() functions may result in a use-after-free scenario, potentially allowing a local user to escalate privileges or crash the system.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCws61975

Cisco IMC includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2015-5477—An error in the handling of TKEY queries in ISC BIND 9 can be exploited by a remote attacker to trigger a REQUIRE assertion failure, causing the named daemon to exit and resulting in a denial of service.
- CVE-2016-2776—A flaw in the way ISC BIND 9 constructs responses to specific queries can lead to an assertion failure in buffer.c, allowing a remote attacker to cause the named process to crash and exit unexpectedly.
- CVE-2023-50387—Known as "KeyTrap," this vulnerability in DNSSEC-validating resolvers (such as BIND and Unbound) allows a remote attacker to cause extreme CPU exhaustion and a denial of service by providing a specially crafted DNSSEC-signed zone with complex resource record combinations.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCws65661

Cisco IMC includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2010-2252—Wget 1.12 and earlier allows remote attackers to write to arbitrary files via a 302 redirect to a URL with a different filename when the -O (output document) option is used, as Wget uses the filename from the redirected URL rather than the original.
- CVE-2014-4877—Wget before 1.16 allows remote FTP servers to write to arbitrary files, and potentially execute code, via a symlink attack in a directory listing during a recursive retrieval.

- CVE-2016-4971—Wget before 1.18 allows remote servers to write to arbitrary files by redirecting an HTTP request to an FTP URL, which causes Wget to save the file with a name provided by the FTP server rather than the original HTTP filename.
- CVE-2017-6508—Wget before 1.19.1 allows remote attackers to inject arbitrary HTTP headers (CRLF injection) via a crafted URL, which could lead to session hijacking or other header-based attacks.
- CVE-2018-0494—Wget before 1.19.5 allows remote attackers to bypass intended cookie access restrictions via a malformed Set-Cookie header, potentially leading to cookie injection or overwriting.
- CVE-2021-31879—Wget before 1.21.1 does not properly handle certain HTTP response headers, such as Content-Length, which may allow a remote attacker to bypass security controls or cause unexpected behavior.
- CVE-2024-10524—A path traversal vulnerability exists in certain versions of WPS Office for Windows that allows an attacker to achieve arbitrary code execution via a specially crafted file.
- CVE-2024-38428—Wget before 1.24.5 is vulnerable to a flaw where it fails to properly parse userinfo in a URI, which could be exploited to bypass security filters or lead to credential disclosure in certain configurations.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCws68419

Cisco IMC includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2009-5155—An off-by-one error in the strfmon_l function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large precision value.
- CVE-2010-0015—The NIS+ implementation in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted NIS+ directory name that triggers a buffer overflow.
- CVE-2011-5320—The tar implementation in BusyBox before 1.20.0 allows remote attackers to create or overwrite arbitrary files via a directory traversal attack in a tar header.
- CVE-2012-4412—An integer overflow in the strcoll function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string.
- CVE-2012-4424—A stack-based buffer overflow in the strcoll function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string.
- CVE-2013-4237—The readdir_r function in the GNU C Library (glibc) does not properly handle certain directory entries, which allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash).
- CVE-2013-4458—A stack-based buffer overflow in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a large number of AF_INET6 addresses.

- CVE-2013-4788—The PTR_MANGLE implementation in the GNU C Library (glibc) does not properly initialize the guard value, which allows local attackers to bypass the pointer-guarding protection mechanism.
- CVE-2014-4043—The posix_spawn_file_actions_addopen function in the GNU C Library (glibc) before 2.20 does not copy its path argument, which allows context-dependent attackers to trigger a use-after-free vulnerability.
- CVE-2014-6040—An out-of-bounds read in the iconv function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a crafted multibyte sequence.
- CVE-2014-7817—The wordexp function in the GNU C Library (glibc) allows context-dependent attackers to execute arbitrary commands via a crafted string that triggers command substitution even when WRDE_NOCMD is specified.
- CVE-2014-8121—The nss_files implementation in the GNU C Library (glibc) does not properly handle certain database files, which allows local attackers to cause a denial of service (infinite loop) or corrupt the database.
- CVE-2014-9402—The getnetbyname function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (infinite loop) via a crafted DNS response.
- CVE-2014-9761—A stack-based buffer overflow in the nan function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a long string.
- CVE-2015-1781—A buffer overflow in the gethostbyname_r function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long hostname.
- CVE-2015-5180—A NULL pointer dereference in the res_query function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted DNS response.
- CVE-2015-8776—An out-of-bounds access in the strftime function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a crafted format string.
- CVE-2015-8777—The LD_POINTER_GUARD environment variable in the GNU C Library (glibc) allows local attackers to bypass the pointer-guarding protection mechanism by disabling it.
- CVE-2015-8778—An integer overflow in the hcreate function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large number of elements.
- CVE-2015-8779—A stack-based buffer overflow in the catopen function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long catalog name.
- CVE-2015-8982—A buffer overflow in the strftime function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a crafted format string.
- CVE-2015-8983—An integer overflow in the _IO_wstr_overflow function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large string.
- CVE-2015-8984—An out-of-bounds read in the fnmatch function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a crafted pattern.

- CVE-2015-8985—The pop_fail_stack function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (assertion failure and crash) via vectors related to extended regular expression processing.
- CVE-2016-10228—An out-of-bounds write in the iconv function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted multibyte sequence.
- CVE-2016-10739—A buffer overflow in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a large number of AF_INET6 addresses.
- CVE-2016-1234—A stack-based buffer overflow in the glob function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long path.
- CVE-2016-3075—A stack-based buffer overflow in the getnetbyname function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted DNS response.
- CVE-2016-3706—A stack-based buffer overflow in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via vectors involving hostent conversion, due to an incomplete fix for CVE-2013-4458.
- CVE-2016-4429—A stack-based buffer overflow in the clntudp_call function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted RPC response.
- CVE-2017-12132—The DNS stub resolver in the GNU C Library (glibc) before 2.26 will solicit large UDP responses when EDNS support is enabled, potentially simplifying off-path DNS spoofing attacks due to IP fragmentation.
- CVE-2017-15670—An off-by-one error in the glob function in the GNU C Library (glibc) before 2.27 leads to a heap-based buffer overflow when processing home directories using the ~ operator followed by a long string.
- CVE-2017-15671—The glob function in the GNU C Library (glibc) before 2.27 could skip freeing allocated memory when processing the ~ operator with a long username, potentially leading to a denial of service (memory leak).
- CVE-2017-16997—The elf/dl-load.c implementation in the GNU C Library (glibc) does not properly handle certain checks, which allows local attackers to bypass security restrictions via a crafted shared object.
- CVE-2017-8804—The memmove and memcpy implementations in the GNU C Library (glibc) for x86_64 do not properly handle overlapping memory regions in certain cases, which allows context-dependent attackers to cause a denial of service (crash) or possibly have other unspecified impact.
- CVE-2018-1000001—A buffer underflow in the realpath function in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted path.
- CVE-2018-11236—An integer overflow in the __vfprintf_internal function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large precision value.
- CVE-2018-6485—An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (glibc) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.

- CVE-2019-1010023—A buffer overflow in the ld.so dynamic loader in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted environment variable.
- CVE-2019-19126—The GNU C Library (glibc) before 2.31 does not properly handle the LD_PRELOAD environment variable for SUID binaries, which allows local attackers to bypass security restrictions.
- CVE-2019-25013—A buffer overflow in the iconv function in the GNU C Library (glibc) when converting to the EUC-KR character set allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.
- CVE-2019-9169—A heap-based buffer overflow in the regexec function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted regular expression.
- CVE-2020-10029—A stack-based buffer overflow in the cosl function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large input value.
- CVE-2020-1751—A stack-based buffer overflow in the _dl_open function in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted shared object path.
- CVE-2020-1752—A use-after-free vulnerability in the glob function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted path.
- CVE-2020-27618—A buffer overflow in the iconv function in the GNU C Library (glibc) when converting to the IBM1364 character set allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.
- CVE-2020-29573—A buffer overflow in the printf function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a large precision value.
- CVE-2021-27645—A double-free vulnerability in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code.
- CVE-2021-3326—A buffer overflow in the iconv function in the GNU C Library (glibc) when converting to the ISO-2022-JP-3 character set allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.
- CVE-2021-33574—A use-after-free vulnerability in the mq_notify function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.
- CVE-2021-35942—A buffer overflow in the wordexp function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a long string.
- CVE-2021-3999—A buffer overflow in the getcwd function in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long path.
- CVE-2022-23218—A stack-based buffer overflow in the svcunix_create function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted RPC request.
- CVE-2022-23219—A stack-based buffer overflow in the clnt_create function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted RPC request.

- CVE-2023-4527—A stack-based buffer overflow in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a large DNS response received over TCP.
- CVE-2023-4806—A use-after-free vulnerability in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted DNS response.
- CVE-2023-4813—A use-after-free vulnerability in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted DNS response.
- CVE-2023-4911—A buffer overflow in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable allows a local attacker to execute arbitrary code with elevated privileges.
- CVE-2023-5156—A memory leak in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (memory exhaustion) via a crafted DNS response.
- CVE-2024-2961—A buffer overflow in the iconv function in the GNU C Library (glibc) when converting to the ISO-2022-CN-EXT character set allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.
- CVE-2024-33599—A buffer overflow in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code.
- CVE-2024-33600—A NULL pointer dereference in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) via a crafted request.
- CVE-2024-33601—A buffer overflow in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code.
- CVE-2024-33602—A buffer overflow in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code.
- CVE-2025-0395—A buffer overflow in the assert() function in the GNU C Library (glibc) versions 2.13 to 2.40 occurs because insufficient space is allocated for the failure message, potentially leading to a denial of service.
- CVE-2025-4802—A vulnerability in the GNU C Library (glibc) versions 2.27 to 2.38 allows a local attacker to load malicious shared libraries and escalate privileges via an untrusted LD_LIBRARY_PATH in statically compiled setuid binaries that call dlopen.
- CVE-2025-5702—A vulnerability in the optimized strcmp implementation for Power10 processors in the GNU C Library (glibc) version 2.39 and later improperly initializes vector registers, potentially leading to data corruption or altered control flow.
- CVE-2025-8058—A double-free vulnerability in the regcomp function in the GNU C Library (glibc) versions 2.4 to 2.41 occurs during bracket expression parsing when a memory allocation failure takes place, potentially allowing arbitrary code execution.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCws68836

Cisco IMC includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2007-5116—A buffer overflow in the polymorphic opcode support in the Regular Expression Engine (regcomp.c) in Perl 5.8 allows context-dependent attackers to execute arbitrary code by switching from byte to Unicode (UTF) characters in a regular expression.
- CVE-2008-1927—A double free vulnerability in Perl 5.8.8 allows context-dependent attackers to cause a denial of service (memory corruption and crash) via a crafted regular expression containing UTF-8 characters.
- CVE-2008-5302—A race condition in the rmtree function in File::Path in Perl 5.8.8 and 5.10.0 allows local users to create arbitrary setuid binaries via a symlink attack.
- CVE-2008-5303—A race condition in the rmtree function in File::Path in Perl 5.8.8 allows local users to delete arbitrary files via a symlink attack, representing a regression of a previous security fix.
- CVE-2010-1168—The Safe (aka Safe.pm) module before 2.25 for Perl allows context-dependent attackers to bypass intended access restrictions and execute arbitrary code via vectors involving implicitly called methods such as DESTROY and AUTOLOAD.
- CVE-2010-1447—The Safe (aka Safe.pm) module 2.26 and earlier for Perl allows context-dependent attackers to bypass access restrictions and execute arbitrary code via vectors involving subroutine references and delayed execution.
- CVE-2010-2761—The multipart_init function in CGI.pm before 3.50 uses a hardcoded MIME boundary string, which allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks.
- CVE-2010-4410—A CRLF injection vulnerability in the header function in CGI.pm before 3.50 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via newline characters.
- CVE-2011-0761—Perl 5.10.x allows context-dependent attackers to cause a denial of service (NULL pointer dereference and crash) by injecting arguments into functions such as getpeername, readdir, and closedir.
- CVE-2011-1487—The lc, lcfirst, uc, and ucfirst functions in Perl 5.10.x through 5.13.x do not apply the taint attribute to return values, allowing attackers to bypass taint protection mechanisms via crafted strings.
- CVE-2011-2939—An off-by-one error in the decode_xs function in the Encode module for Perl allows context-dependent attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted Unicode string.
- CVE-2011-3597—An eval injection vulnerability in the Digest module before 1.17 for Perl allows context-dependent attackers to execute arbitrary commands via the new constructor.
- CVE-2011-4116—The _is_safe function in the File::Temp module for Perl does not properly handle symlinks, which could allow a local attacker to bypass security checks.
- CVE-2012-5195—A heap-based buffer overflow in the Perl_repeatcpy function in Perl allows context-dependent attackers to cause a denial of service or execute arbitrary code via the 'x' string repeat operator.
- CVE-2012-5526—CGI.pm before 3.63 for Perl does not properly escape newlines in Set-Cookie or P3P headers, allowing remote attackers to inject arbitrary headers into HTTP responses.

- CVE-2012-6329—The Locale::Maketext implementation in Perl before 5.17.7 does not properly handle backslashes and method names, allowing context-dependent attackers to execute arbitrary commands via crafted translation strings.
- CVE-2013-1667—The rehash mechanism in Perl 5.8.2 through 5.16.x allows context-dependent attackers to cause a denial of service (memory consumption and crash) via a crafted hash key.
- CVE-2013-7422—An integer underflow in the regular expression engine (regcomp.c) in Perl before 5.20 allows context-dependent attackers to execute arbitrary code or cause a denial of service via long digit strings.
- CVE-2014-4330—The Dumper method in Data::Dumper before 2.154 allows context-dependent attackers to cause a denial of service (stack exhaustion and crash) via deeply nested Array-References.
- CVE-2015-8853—The regular expression engine in Perl before 5.24.0 allows context-dependent attackers to cause a denial of service (infinite loop and high CPU usage) via crafted UTF-8 data.
- CVE-2016-1238—Perl 5.x before 5.22.3 and 5.24.1 does not properly remove the current directory (".") from the module include path (@INC), allowing local users to gain privileges via a Trojan horse module.
- CVE-2016-2381—Perl might allow context-dependent attackers to bypass the taint protection mechanism in a child process via duplicate environment variables in the envp array.
- CVE-2016-6185—The XSLoader::load method in Perl does not properly locate shared object (.so) files when called in a string eval, potentially allowing local users to execute arbitrary code via a malicious library.
- CVE-2018-12015—The Archive::Tar module in Perl through 5.26.2 allows remote attackers to bypass directory-traversal protection and overwrite arbitrary files via an archive containing a symlink and a regular file with the same name.
- CVE-2018-18311—Perl before 5.26.3 and 5.28.1 has a buffer overflow vulnerability via a crafted regular expression that triggers invalid write operations.
- CVE-2018-6913—A heap-based buffer overflow in the pack function in Perl before 5.26.2 allows context-dependent attackers to execute arbitrary code via a large item count.
- CVE-2020-10543—Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.
- CVE-2020-10878—Perl before 5.30.3 has an integer overflow related to mishandling of specific instructions in the regular expression engine, potentially leading to instruction injection.
- CVE-2020-12723—A buffer overflow vulnerability in the regular expression compiler (regcomp.c) in Perl before 5.30.3 occurs during recursive calls to S_study_chunk.
- CVE-2020-16156—CPAN 2.28 allows a signature verification bypass, which could allow an attacker to bypass security checks for Perl modules downloaded from the network.
- CVE-2023-31484—CPAN.pm before 2.35 and Perl before 5.38.0 do not verify TLS certificates when downloading distributions over HTTPS, exposing users to man-in-the-middle attacks.
- CVE-2023-47038—A heap-based buffer overflow vulnerability was found in Perl 5.30.0 through 5.38.0 when compiling a crafted regular expression with illegal Unicode properties.
- CVE-2024-56406—A heap buffer overflow vulnerability in Perl's tr operator occurs when processing non-ASCII bytes, potentially leading to a denial of service or arbitrary code execution.

- CVE-2025-40909—A race condition in Perl threads during directory handle cloning can cause the current working directory to change unexpectedly, potentially allowing a local attacker to trick threads into loading malicious code.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwr84274

Cisco IMC includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2025-27363—An out-of-bounds write vulnerability in FreeType versions 2.13.0 and below occurs when parsing font subglyph structures in TrueType GX and variable font files; improper data type assignment leads to a buffer wraparound and undersized heap allocation, potentially allowing arbitrary code execution.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwr84317

Cisco IMC includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2023-38545—A high-severity heap-based buffer overflow vulnerability in curl's SOCKS5 proxy handshake occurs when a hostname longer than 255 bytes is incorrectly copied into a target buffer during a slow handshake, potentially allowing a malicious proxy to execute arbitrary code on the client.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwq11344

Cisco IMC includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-1999-0289—The Apache web server for Win32 may provide access to restricted files when a dot (.) is appended to a requested URL, potentially allowing unauthorized file disclosure.
- CVE-1999-0678—A default configuration of Apache on Debian GNU/Linux sets the ServerRoot to /usr/doc, which allows remote users to read documentation files for the entire server.
- CVE-2010-1151—A race condition in the mod_auth_shadow module for the Apache HTTP Server allows remote attackers to bypass authentication and read or modify data via improper interaction with an external helper application.
- CVE-2023-31122—An out-of-bounds read vulnerability in the mod_macro module of Apache HTTP Server versions through 2.4.57 allows an attacker to cause a crash or obtain sensitive information when processing long macros.
- CVE-2023-38709—Faulty input validation in the core of Apache HTTP Server through version 2.4.58 allows malicious or exploitable backend content generators to split HTTP responses, potentially leading to cache poisoning or XSS.

- CVE-2023-43622—A flaw in the mod_http2 module allows an attacker opening an HTTP/2 connection with an initial window size of 0 to block handling of that connection indefinitely, exhausting worker resources in a "slow loris" style attack.
- CVE-2023-45802—When an HTTP/2 stream is reset by a client, memory resources may not be reclaimed immediately, allowing a client to grow the server's memory footprint and potentially cause a denial of service.
- CVE-2024-24795—An HTTP response splitting vulnerability in multiple Apache HTTP Server modules allows an attacker to inject malicious response headers into backend applications, leading to HTTP desynchronization attacks.
- CVE-2024-27316—The Apache HTTP Server fails to limit the amount of HTTP/2 CONTINUATION frames sent within a single stream, which can lead to memory exhaustion and a denial of service condition.
- CVE-2024-36387—Serving WebSocket protocol upgrades over an HTTP/2 connection in Apache HTTP Server could result in a null pointer dereference, leading to a crash of the server process.
- CVE-2024-38472—A Server-Side Request Forgery (SSRF) vulnerability in Apache HTTP Server on Windows allows an attacker to potentially leak NTLM hashes to a malicious server via crafted requests or content.
- CVE-2024-38473—An encoding problem in the mod_proxy module allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests.
- CVE-2024-38474—A substitution encoding issue in mod_rewrite allows an attacker to execute scripts in directories permitted by configuration but not directly reachable by URL, or disclose script source code meant only for CGI execution.
- CVE-2024-38475—Improper escaping of output in mod_rewrite allows an attacker to map URLs to filesystem locations that are permitted to be served but are not intended to be directly reachable, potentially resulting in code execution.
- CVE-2024-38476—Vulnerabilities in the core of Apache HTTP Server allow information disclosure, SSRF, or local script execution via backend applications whose response headers are malicious or exploitable.
- CVE-2024-38477—A null pointer dereference in the mod_proxy module of Apache HTTP Server allows an attacker to crash the server via a specially crafted malicious request.
- CVE-2024-39573—A potential SSRF vulnerability in mod_rewrite allows an attacker to cause unsafe RewriteRules to unexpectedly set up URLs to be handled by mod_proxy, bypassing intended access controls.
- CVE-2024-40898—An SSRF vulnerability in Apache HTTP Server on Windows with mod_rewrite in server/vhost context allows potential leakage of NTLM hashes to a malicious server via crafted requests.
- CVE-2025-3891—A flaw in the mod_auth_openidc module for Apache HTTP Server allows a remote attacker to trigger a denial of service by sending an empty POST request when the OIDCPreservePost directive is enabled.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCws68830

Cisco IMC includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2005-3962—An integer overflow in the format string functionality (Perl_sv_vcatpvfn) in Perl 5.8.6 and 5.9.2 allows attackers to overwrite arbitrary memory or execute arbitrary code via format string specifiers with large values.
- CVE-2005-4278—An untrusted search path vulnerability in Perl before 5.8.7-r1 on Gentoo Linux allows local users in the portage group to gain privileges via a malicious shared object in the Portage temporary build directory.
- CVE-2007-5116—A buffer overflow in the polymorphic opcode support in the Regular Expression Engine (regcomp.c) in Perl 5.8 allows context-dependent attackers to execute arbitrary code by switching from byte to Unicode characters in a regular expression.
- CVE-2010-1158—An integer overflow in the regular expression engine in Perl 5.8.x allows context-dependent attackers to cause a denial of service (stack consumption and crash) by matching a crafted regular expression against a long string.
- CVE-2011-2728—The bsd_glob function in the File::Glob module for Perl before 5.14.2 allows context-dependent attackers to cause a denial of service (crash) via a glob expression with the GLOB_ALTDIRFUNC flag, triggering an uninitialized pointer dereference.
- CVE-2011-2939—An off-by-one error in the decode_xs function in the Encode module for Perl allows context-dependent attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted Unicode string.
- CVE-2012-6329—The Locale::Maketext implementation in Perl before 5.17.7 does not properly handle backslashes and method names, allowing context-dependent attackers to execute arbitrary commands via crafted translation strings.
- CVE-2013-1667—The rehash mechanism in Perl 5.8.2 through 5.16.x allows context-dependent attackers to cause a denial of service (memory consumption and crash) via a crafted hash key.
- CVE-2014-4330—The Dumper method in Data::Dumper before 2.154 allows context-dependent attackers to cause a denial of service (stack exhaustion and crash) via deeply nested Array-References.
- CVE-2015-8853—The regular expression engine in Perl before 5.24.0 allows context-dependent attackers to cause a denial of service (infinite loop and high CPU usage) via crafted UTF-8 data.
- CVE-2016-1238—Perl 5.x before 5.22.3 and 5.24.1 does not properly remove the current directory (".") from the module include path (@INC), allowing local users to gain privileges via a Trojan horse module.
- CVE-2016-2381—Perl might allow context-dependent attackers to bypass the taint protection mechanism in a child process via duplicate environment variables in the envp array.
- CVE-2017-12814—A stack-based buffer overflow in the CPerlHost::Add method in win32/perlhost.h in Perl before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 on Windows allows attackers to execute arbitrary code via a long environment variable.
- CVE-2017-12837—A heap-based buffer overflow in the S_regatom function in regcomp.c in Perl before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to cause a denial of service via a regular expression with a \N{} escape and the case-insensitive modifier.

- CVE-2017-12883—A buffer overflow in the S_grok_bslash_N function in regcomp.c in Perl before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to disclose sensitive information or cause a denial of service via a crafted regular expression with an invalid \N{U+...} escape.
- CVE-2018-12015—The Archive::Tar module in Perl through 5.26.2 allows remote attackers to bypass directory-traversal protection and overwrite arbitrary files via an archive containing a symlink and a regular file with the same name.
- CVE-2018-18311—An integer overflow in the Perl_my_setenv function in Perl before 5.26.3 and 5.28.1 allows local attackers to cause a denial of service or execute arbitrary code via a large environment variable.
- CVE-2018-18312—A heap-based buffer overflow in the S_handle_regex_sets function in regcomp.c in Perl before 5.26.3 and 5.28.1 allows remote attackers to cause a denial of service or execute arbitrary code via a crafted regular expression.
- CVE-2018-18313—A heap-based buffer read overflow in the S_grok_bslash_N function in regcomp.c in Perl before 5.26.3 and 5.28.1 allows remote attackers to disclose sensitive information from process memory via a crafted regular expression.
- CVE-2018-18314—A heap-based buffer overflow in the S_regatom function in regcomp.c in Perl before 5.26.3 and 5.28.1 allows remote attackers to cause a denial of service or execute arbitrary code via a crafted regular expression.
- CVE-2018-6913—A heap-based buffer overflow in the pack function in Perl before 5.26.2 allows context-dependent attackers to execute arbitrary code via a large item count.
- CVE-2020-10543—Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.
- CVE-2020-10878—Perl before 5.30.3 has an integer overflow related to mishandling of specific instructions in the regular expression engine, potentially leading to instruction injection.
- CVE-2020-12723—A buffer overflow vulnerability in the regular expression compiler (regcomp.c) in Perl before 5.30.3 occurs during recursive calls to S_study_chunk.
- CVE-2022-48522—A stack-based crash (infinite recursion) in the S_find_uninit_var function in Perl 5.34.0 occurs when attempting to print warning messages, potentially leading to a denial of service.
- CVE-2023-31484—CPAN.pm before 2.35 and Perl before 5.38.0 do not verify TLS certificates when downloading distributions over HTTPS, exposing users to man-in-the-middle attacks.
- CVE-2023-31486—HTTP::Tiny before 0.083, a Perl core module, has an insecure default TLS configuration where users must opt in to verify certificates, potentially exposing applications to man-in-the-middle attacks.
- CVE-2023-47039—A binary hijacking vulnerability in Perl for Windows occurs because it relies on the system path to find the shell (cmd.exe) and initially searches the current working directory, allowing local privilege escalation.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Resolved Caveats

Resolved Caveats in Release 6.0(2.260044)

The following defects were resolved in Release 6.0(2.260044):

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCws30219	Cisco UCS M7 servers may experience hostlockups due to ECC errors during runtime. The BIOS fails to retrieve a variable properly, causing EFI to return an invalid parameter, which leads to the host freezing without any logs or Cisco IMC alerts.The host becomes unresponsive, and KVM input is not accepted. This issue is resolved.	4.3(6.250053)	6.0(2.260044)
CSCws62117	Cisco UCS C240-M8 server with LPe35002-M2 Emulex adapters connected to Brocade SAN switches and Dellstorage arrays experience intermittent I_T NexusLoss errors, causing unstable connections and periodic LUN disconnections. Although FCP I/O completes without errors, the adapter repeatedly attempts to re-establish the connection by issuing LOGO and FLOGI commands, which temporarily restore connectivity before the issue recurs. This issue is resolved.	4.3(6.250053)	6.0(2.260044)

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwq55604	DIMM_P2_H1 on all Cisco UCS C245 M8 integrated servers reports as inoperable, although all DIMMs function correctly with no memory errors.The issue triggers alerts indicating equipment inoperability and incompatible server firmware, despite the server being fully populated with supported identical DIMM models. This issue is resolved.	4.3(5.250001)	6.0(2.260044)
CSCwr82017	Cisco UCS C220 M8 server and C240 M8 server will continuously reset if the Intel SGX Processor Reserved Memory Range Registers (PRMRR) size is configured to an unsupported size in the system memory settings. This issue is resolved.	6.0(1.250192)	6.0(2.260044)
CSCwr45526	Certain Cisco UCS servers experience boot interruptions caused by validation failures in the Secure Boot database. This issue affects specific server models during system startup, leading to potential boot interruptions and impacting system reliability. The problem arises from outdated certificates in the Secure Boot database that prevent successful secure boot processes. This issue is resolved.	4.3(6.260017)	6.0(2.260044)

Open Caveats

Open Caveats in Release 6.0(2.260044)

The following defects are open in Release 6.0(2.260044):

Defect ID	Symptom	Workaround	First Affected Release
CSCwt41941	On Cisco UCS C220 and C240 M8 servers, firmware versions using Intel Secondary Service Processor (SSP) 2.0 are not backward compatible with earlier releases using SSP 1.6. The firmware versions that support SSP 2.0 are: 4.3(6.260003), 6.0(1.250192), 6.0(2.260044) or later Downgrading to an earlier version causes the Baseboard Management Controller (BMC) to fail BIOS attestation, leading to critical system instability. Symptoms include systems getting stuck in the KVM console, boot failures, POST hangs, Catastrophic Error (CATERR) events, inoperable NVMe devices, and temperature sensor failures along with critical thermal threshold errors.	If you downgrade to an earlier firmware version and BMC fails, use the following recovery steps: **1.** Upgrade BMC Firmware: Use the Host Software Upgrade (HSU) or the Cisco IMC interface to upgrade only the BMC firmware component to the latest version (SSP 2.0 compatible). **2.** Perform a Host Power Reset: A full host power reset may help recover the system state, though it is not guaranteed to be 100% effective in all scenarios.	• 4.3(6.260003) • 6.0(1.250192) • 6.0(2.260044)

Known Behaviour and Limitations

Known Behaviors and Limitations in Release 6.0(2.260044)

The following caveats are known limitations in release 6.0(2.260044):

Defect ID	Symptom	Workaround	First Affected Release
CSCwt34870	Users may experience failures when executing `snmpget` commands for enterprise OIDs (.1.3.6.1.4.1.9.9.719). Furthermore, if an `snmpget` command fails for these specific OIDs, subsequent `snmpwalk` operations may also fail. This issue is observed after upgrading to the release version 6.0(2.260044).	Refrain from executing `snmpget` commands on the enterprise OIDs (.1.3.6.1.4.1.9.9.719). If an `snmpget` command has already been executed and subsequent `snmpwalk` operations are failing, you may restore SNMP functionality by performing one of the following actions: • Perform a Cisco IMC reboot. • Disable and re-enable the SNMP service.	6.0(2.260044)

CSCwr72707	A significant drop in random workload performance is observed on NVMe drives when multiple drives (more than two) are populated and tested concurrently on Cisco UCS C220 M8 systems with Red Hat Enterprise Linux (RHEL) OS. Specifically, 4K random read performance may drop from a rated 1,600k IOPS per drive to approximately 680k IOPS per drive during concurrent operations.	To resolve this performance bottleneck, apply the following Intel-recommended kernel tuning parameters in the RHEL boot configuration:
		• For Single-Drive Configurations: Add the following to the RHEL kernel command line:
		`intel_pstate=disable pcie_aspm.policy=performance pci=pcie_bus_safe`
		• For Multi-Drive (Fully Populated) Configurations: Add the following to the RHEL kernel command line:
		`intel_pstate=disable pcie_aspm.policy=performance pci=pcie_bus_safe nvme.poll_queues=32 intel_iommu=on`
			6.0(2.260044)

Supported Platforms and Release Compatibility Matrix

Supported Platforms in this Release

The following servers are supported in this release:

- Cisco UCS C220 M8
- Cisco UCS C240 M8
- Cisco UCS C225 M8
- Cisco UCS C245 M8
- Cisco UCS C220 M7
- Cisco UCS C240 M7
- Cisco UCS C220 M6
- Cisco UCS C240 M6
- Cisco UCS C225 M6
- Cisco UCS C245 M6

For information about these servers, see Overview of Servers.

Cisco IMC and Cisco UCS Manager Release Compatibility Matrix

Firmware Version Equivalency Between Cisco Intersight, Cisco IMC, and Cisco UCS Manager

For more information, see Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager.

Cisco IMC and Cisco UCS Manager Release Compatibility Matrix

Cisco UCS C-Series Rack-Mount Servers are managed by built-in standalone software —Cisco IMC. However, when a Rack-Mount Server is integrated with Cisco UCS Manager, UCSM end-user interface is used to manage the server.

The following table lists the supported platforms, Cisco IMC releases, and Cisco UCS Manager releases for Rack-Mount Servers:

Table 1: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 6.0(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
6.0(2.260044)	6.0(2b)	• Cisco UCS C220 M8, C240 M8, C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers

Table 2: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 6.0(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
6.0(1.250194)	NA	• Cisco UCS C220 M8 servers
6.0(1.250192)	6.0(1e)	• Cisco UCS C220 M8, C240 M8, C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers
6.0(1.250174)	6.0(1d)	• Cisco UCS C220 M8, C240 M8, C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers
6.0(1.250131)	6.0(1c)	• Cisco UCS C220 M8, C240 M8, C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
6.0(1.250130)	6.0(1b)	• Cisco UCS C245 M8 servers
6.0(1.250127)		• Cisco UCS C220 M8, C225 M8 and C240 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers

Table 3: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(6) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(6.260017)	4.3(6f)	• Cisco UCS C220 M8, C225 M8, C240 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS S3260 M5 servers
4.3(6.260003)	4.3(6e)	• Cisco UCS C220 M8 and C240 M8 servers • Cisco UCS C220 M7 and C240 M7 servers
4.3(6.250117)	NA	• Cisco UCS C220 M7 servers
4.3(6.250101)	4.3(6d)	• Cisco UCS C220 M8, C225 M8, C240 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS S3260 M5 servers
4.3(6.250060)	NA	• Cisco UCS C245 M8 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(6.250053)	4.3(6c)	• Cisco UCS C220 M8, C225 M8, C240 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS S3260 M5 servers
4.3(6.250044)	4.3(6b)	• Cisco UCS C220 M8, C225 M8, C240 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers
4.3(6.250039)	4.3(6a)	• Cisco UCS C220 M8 and C240 M8 servers • Cisco UCS S3260 M5 servers
4.3(6.250040)		• Cisco UCS C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers

Table 4: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(5) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(5.250045)	NA	• Cisco UCS C225 M8 servers
4.3(5.250043)	NA	• Cisco UCS C225 M8 and C245 M8 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(5.250033)	NA	• Cisco UCS C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6, C245 M6 servers and S3260 M5 servers
4.3(5.250030)	4.3(5d)	• Cisco UCS C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6, C245 M6 servers and S3260 M5 servers
4.3(5.250001)	4.3(5c)	• Cisco UCS C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6, C245 M6 servers and S3260 M5 servers
4.3(5.240021)	4.3(5a)	• Cisco UCS C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6, C245 M6 servers and S3260 M5 servers

Table 5: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(4) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
• 4.3(4.252002) • 4.3(4.252001)	NA	• 4.3(4.252002) - Cisco UCS C225 M6 servers • 4.3(4.252001) - Cisco UCS C220 M6, C240 M6 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(4.242066)	4.3(4f)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 and S3260 M5 servers
4.3(4.242038)	NA	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 and S3260 M5 servers
4.3(4.242028)	NA	• Cisco UCS C220 M7 and C240 M7 servers
4.3(4.241063)	4.3(4b)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 and S3260 M5 servers
4.3(4.241014)	4.3(4b)	Cisco UCS C245 M8 server
4.3(4.240152)	4.3(4a)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 and S3260 M5 servers

Table 6: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(3.240043)	NA	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers
4.3(3.240041)	NA	• Cisco UCS S3260 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(3.240022)	4.3(3a)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 and S3260 M5 servers

Table 7: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(2.260007)	4.3(6f)	Cisco UCS C220 M5, C240 M5, C480 M5 and C125 M5 servers
4.3(2.250063)	NA	Cisco UCS C220 M5, C240 M5, C480 M5 and C125 M5 servers
4.3(2.250045)	NA	Cisco UCS C220 M5, C240 M5, C480 M5 and C125 M5 servers
4.3(2.250037)	4.3(6c)	Cisco UCS C220 M5, C240 M5, C480 M5 servers
4.3(2.250022)	NA	Cisco UCS C125 M5 servers
4.3(2.250021)	NA	Cisco UCS C240 M5 servers
4.3(2.250016)	NA	Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.240107)	NA	Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.240090)	NA	Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.240077)	NA	Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.240053)	NA	Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.240037)	NA	• Cisco UCS C225 M6 and C245 M6 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(2.240009)	NA	• Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.240002)	4.3(2)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.230270)	4.3(2)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.230207)	4.3(2)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers

Table 8: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(1.230138)	No Support	Cisco UCS C220 M7 and C240 M7 servers
4.3(1.230124)	No Support	Cisco UCS C220 M7 and C240 M7 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(1.230097)	No Support	Cisco UCS C220 M7 and C240 M7 servers

Table 9: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.2(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(3p)	4.2(3o)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5, and C125 M5 servers
4.2(3o)	4.2(3n)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3n)	4.2(3m)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3m)	4.2(3l)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3l)	4.2(3k)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3k)	NA	Cisco UCS S3260 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(3j)	4.2(3j)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3i)	4.2(3i)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3g)	4.2(3g)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3e)	4.2(3e)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3d)	4.2(3d)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3b)	4.2(3b)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers

Table 10: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.2(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(2g)	4.2(2d)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(2f)	4.2(2c)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(2a)	4.2(2a)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers

Table 11: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.2(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(1j)	4.2(1n)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1i)	4.2(1m)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1g)	No Support	Cisco UCS C225 M6 and C245 M6 servers
4.2(1f)	4.2(1k)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1e)	4.2(1i)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1c)	No Support	Cisco UCS C225 M6 and C245 M6 servers
4.2(1b)	4.2(1f)	Cisco UCS C220 M6 and C240 M6 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(1a)	4.2(1d)	Cisco UCS C220 M6, C240 M6, and C245 M6 servers **Note** Cisco UCS Manager does not support Cisco UCS C245 M6 servers.

Table 12: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.1(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(3n)	NA	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and S3260 M4 servers
4.1(3m)	4.1(3m)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and S3260 M4 servers
4.1(3l)	4.1(3k)	Cisco UCS C480 M5, C220 M5, C240 M5 servers
4.1(3i)	4.1(3j)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5 servers
4.1(3h)	4.1(3i)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5 servers
4.1(3g)	No Support	Cisco UCS S3260 M4 and S3260 M5 servers
4.1(3f)	4.1(3h)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M4, S3260 M5, and C125 M5 servers
4.1(3d)	4.1(3e)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.1(3c)	4.1(3d)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5 and C125 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(3b)	4.1(3a)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5 and C125 M5 servers

Table 13: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.1(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(2m)	No Support	Cisco UCS C220 M4, C240 M4 and C460 M4 servers.
4.1(2l)	No Support	Cisco UCS C220 M4 and C240 M4 servers.
4.1(2k)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2j)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2h)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2g)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2f)	4.1(2c)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(2e)	No Support	Cisco UCS C125 M5 servers
4.1(2d)	No Support	Cisco UCS C240 M5 and C240 SD M5 servers
4.1(2b)	4.1(2b)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(2a)	4.1(2a)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers

Table 14: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.1(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(1h)	4.1(1e)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(1g)	4.1(1d)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(1f)	4.1(1c)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(1d)	4.1(1b)	Cisco UCS C220 M5, C240 M5, C480 M5, and C480 ML M5 servers
4.1(1c)	4.1(1a)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers

Firmware Files

Firmware Files

The C-Series software release version 6.0(2.260044) includes the following software files:

CCO Software Type	File name(s)	Comment
Unified Computing System (UCS) Server Firmware	For release specific ISO versions, see Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 6.0.	Host Upgrade Utility
Unified Computing System (UCS) Drivers	ucs-cxxx-drivers.6.0(2.260044).iso ucs-cxxx-drivers.6.0(2.260044).iso	Drivers
Unified Computing System (UCS) Utilities	ucs-cxxx-utils-efi.6.0(2.260044).iso ucs-cxxx-utils-linux.6.0(2.260044).iso ucs-cxxx-utils-vmware.6.0(2.260044).iso ucs-cxxx-utils-windows.6.0(2.260044).iso	Utilities

Note Always upgrade the BIOS, the Cisco IMC and CMC from the HUU ISO. Do not upgrade individual components (only BIOS or only Cisco IMC), since this could lead to unexpected behavior. If you choose to upgrade BIOS, and the Cisco IMC individually and not from the HUU ISO, make sure to upgrade both Cisco IMC, and BIOS to the same container release.

If the BIOS and the Cisco IMC versions are from different container releases, it could result in unexpected behavior. Cisco recommends that you use the Update All option from the Host Upgrade Utility to update the firmware versions of Cisco IMC, BIOS, and all other server components (VIC, RAID Controllers, PCI devices, and LOM) together.

Host Upgrade Utility

The Cisco Host Upgrade Utility (HUU) is a tool that upgrades the Cisco UCS C-Series firmware.

The image file for the firmware is embedded in the ISO. The utility displays a menu that allows you to choose which firmware components to upgrade. For more information on this utility, see http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

For details of firmware files in Cisco Host Upgrade Utility for individual releases, see Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 6.0.

Updating the Firmware

Use the Host Upgrade Utility to upgrade the C-Series firmware. Host Upgrade Utility can upgrade the following software components:

- BIOS
- Cisco IMC
- CMC
- Cisco VIC Adapters
- Broadcom Adapters
- LAN on Motherboard
- PCIe adapter firmware
- HDD firmware
- SAS Expander firmware
- DCPMM Memory
- PCI Gen5 retimer

All firmware should be upgraded together to ensure proper operation of your server.

Note We recommend that you use the select all and **Update** or **Update & Activate All** option from the Host Upgrade Utility to update the firmware versions of Cisco IMC, BIOS and all other server components (VIC, RAID Controllers, PCI devices, and LOM) together. Click **Exit** once you deploy the firmware.

For more information on how to upgrade the firmware using the utility, see:

http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-user-guide-list.html

Supported Hardware and Software

Operating System and Browser Requirements

For detailed information about supported Operating System, see the interactive UCS Hardware and Software Compatibility matrix.

Cisco recommends the following browsers for Cisco UCS Rack Server Software, Release 6.0(2):

Recommended Browser	Minimum Recommended Browser Version	Minimum Recommended Operating System
Google Chrome	Version 143.0.7499.193 (Official Build) (arm64)	Mac OS 26.2
	Version 143.0.7499.193	Microsoft Windows 11 (10.0.26200)
	Version 143.0.7499.193	Microsoft Windows 11 (26200.7462)
	Microsoft Edge Version 143.0.3650.139 (Official build) (64-bit)	
Safari	Version 26.2 (21623.1.14.11.9)	Mac OS 26.2
	Version 26.2 (21623.1.14.11.9)	
Mozilla Firefox	Version 146.0.1 (aarch64)	
	Version 146.0.1	Microsoft Windows 11 (10.0.26200)
Microsoft Edge	Version 143.0.3650.139	

Note If the management client is launched using an unsupported browser, check the help information from the `For best results use supported browsers` option available in the login window for the supported browser versions.

Transport Layer Security (TLS) version 1.3.

Default Ports

Following is a list of server ports and their default port numbers:

Table 15: Server Ports

Port Name	Port Number
LDAP Port 1	389
LDAP Port 2	389
LDAP Port 3	389
LDAP Port 4	3268
LDAP Port 5	3268
LDAP Port 6	3268
SSH Port	22
HTTP Port	80
HTTPS Port	443
SMTP Port	25
KVM Port	2068
Intersight Management Port	8889
Intersight Cloud Port	8888
SOL SSH Port	2400
SNMP Port	161
SNMP Traps	162
External Syslog	514

Upgrade Paths to Release 6.0(2)

To get a complete overview of all the possible upgrade paths in Cisco IMC, see Cisco UCS Rack Server Upgrade Support Matrix.

SNMP

The supported MIB definition for this release and later releases can be found at the following link:

https://cisco.github.io/cisco-mibs/

Software Utilities

The following standard utilities are available:

- Host Update Utility (HUU)
- BIOS and Cisco IMC Firmware Update utilities

- Server Configuration Utility (SCU)
- Server Diagnostic Utility (SDU)

The utilities features are as follows:

- Availability of HUU, SCU on the USB as bootable images. The USB also contains driver ISO, and can be accessed from the host operating system.

Related Documentation

For configuration information for this release, refer to the following:

- Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide
- Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
- Cisco UCS Rack-Mount Servers Cisco IMC API Programmer's Guide

For information about installation of the C-Series servers, refer to the following:

- Cisco UCS C-Series Rack Servers Install and Upgrade Guides

The following related documentation is available for the Cisco Unified Computing System:

- Regulatory Compliance and Safety Information for Cisco UCS
- For information about supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Refer to the release notes for Cisco UCS Manager software and the *Cisco UCS C Series Server Integration with Cisco UCS Manager Guide* at the following locations:

- Cisco UCS Manager Release Notes
- Cisco UCS C Series Server Integration with Cisco UCS Manager Guides